## The National Conference on Learning and Teaching in Cybersecurity

### 15 June 2016

### Maple House Conference and Training Venue, Birmingham

# Submission Form

DEADLINE FOR SUBMISSION: 27th May, 2016

**Please email the completed form to Dr Kifayat, Kashif** **K.Kifayat@ljmu.ac.uk****.**

**Section 1: Contact details**

|  |  |  |  |
| --- | --- | --- | --- |
| Title:Dr | Given name(s):Chitra | Family name:Balakrishna | Job title:Senior Lecturer |
| Institution/Organisation: Edge Hill UniversityAffiliation:  | HEA Fellowship reference no:FHEA,  |
| Contact address: St. Helen’s Road, Ormskirk, L39 4QP.This is my work Address (delete as appropriate) |
| Email:balakris@edgehill.ac.uk | Twitter name:Chitra\_garge | Telephone:01695657389 |
| Biography for inclusion in the online conference programme and app:Chitra Balakrishna is a Senior Lecturer in Computing at Edge Hill University. She has over 16 years of experience spanning across academia and industry in the areas of Data Networking, Cyber Security, Mobile Communications, Technologies and Applications. In the past she has held academic positions at the University of South Wales prior to joining Edge Hill University in January 2013.Her areas of expertise are Internet of Things, Smart Cities and Applications and Gamification of Cyber education. She has been part of ERDF and FP7 project in the past and currently holds a grant from HEA. She has authored a popular book on IP Multimedia Subsystem by the John Wiley publications in 2009 and has several academic publications to her credit. She has co-founded the prestigious international academic conference and chairs an international workshop on Smart Cities and Application. |

**Section 2: Proposed presentation
Title of session:**

Gamified Virtual Training Environment for Attacker-centric Cyber-security Skills Development

**Please indicate the topic which is most appropriate for your proposed session:**

|  |  |  |  |
| --- | --- | --- | --- |
| Future-oriented cyber security teaching and learning | Χ | Assessment |  |
| Best practices |  | Collaborative learning and social networks |  |
| Social and organisational perspectives |  | Student engagement |  |
| High-impact practices in cyber security learning |  | Learning analytics |  |
| Teaching/educational models, frameworks and platforms |  | Virtual learning environments |  |
| Educational leadership |  | Indigenous, ethnic and cultural perspectives on cyber security teaching |  |
| Curriculum development |  | Engagement with and demand from industry |  |
| Mobile learning |  | Other (please state) |  |

**Please indicate your preferred type of session:**

|  |  |
| --- | --- |
| Paper presentation (30 minutes) | **Χ** |
| Poster |  |
| Interactive Workshop (45 or 60 minutes) |  |
| ‘Demonstration…’ presentation (30 minutes) |  |

**Abstract (up to 150 words): The 150-word abstract should set out the aims and objectives of the session and will be used in the online conference programme and app:**

The findings of the latest cyber security status report by ISACA indicates

shortage of cyber-security professionals is universal and ongoing [1]. A further study conducted by the Ministry of Universities and Science[2] has identified a skills gap that exists amongst the fresh cyber-security graduates, who often do not possess the ability to apply their skills to real-world scenarios as employers demand. Effective cyber-security education unlike most other technical subjects not just requires a hands-on, real-world learning environment but also demands a change of behaviour amongst the learners [2].

CyberGaTE, the HEA funded project aims to bridge the skill-gap between theory and practice as well as address the specific needs of effective cyber-security training through innovative pedagogical practices such as gamification, attacker-centric challenge-based learning.

**Extended abstract (up to 1000 words):**

Gamification is defined as applying game mechanics in a non-gaming context; Game players regularly exhibit persistence, risk-taking, attention to detail and problem solving; behaviours that are ideally suited for effective cyber-security training[3].

An effective cyber-security training calls for change of behaviour; the understanding of how different people perceive risks is critical to effective training. Changing behaviour requires more than providing information about risks and reactive behaviours [5][6]. Most existing gamified training programs use defensive strategies, in line with the current dominant practice in cybersecurity to react, largely, to attacks and not engage in anticipatory or offensive strategies. Moreover, there is a general lack of attacker-centricity, the characteristics of attackers are seldom incorporated in training in order to understand these attackers or anticipate their attacks.

The objective of CyberGaTE is to develop a holistic cyber-security training environment that enables the change in learner’s behaviour by making them security conscious for every action they perform in the real-world environment. This would be achieved by

* Creating challenge-based, ‘think like a hacker’ –type learning resources that would be gamified. Some gaming techniques that shall be explored are real-life problem-based storytelling that would form the basis of the learning content and the use of characters (avatar/role play) and the use of narrative to create a bond between the learner and the avatar thereby enhancing engagement as suggested by literature[4]. CyberGaTE aims to use the known characteristics of cyber-attackers to train participants in anticipating an attacker's motivation and behaviour in carrying out certain attacks. This anticipation enhances the creation and application of both offensive and defensive strategies against cyber-attacks.
* These gamified learning resources would be hosted on a virtual training environment using the innovative concept of ‘Classroom as a Service’, offering the required hands-on real-world experience. The environment incorporating various elements of real-life scenarios would have learners active participants. These scenarios will be live/real-life in the sense of providing active and real time feedback to the learners, on their actions, evaluate them and suggest corrections. In a sense, the learners will be hand-held initially and with increasing learning, they will be evaluated for their actions in the scenarios presented to them for their learning.

The project aims to address issues of engagement and motivation through the use of game mechanics and gamification techniques and by selecting the appropriate gamification elements to suit individual learner needs, thereby aiding in a change of behaviour. Some gaming techniques that shall be explored are real-life problem-based storytelling that would form the basis of the training content to keep the learner motivated. Use of characters (avatar/role play) is known to influence behaviour and the use of narrative to create a bond between the learner and the avatar reinforces the learning and enhances engagement.

The project aims to engage employers and students to build and assess CyberGaTE’s effectiveness as well as disseminate good practice in industry and academia. Overall life-cycle of the project and student-engagement is shown in the illustration below.



**References:**

[1] ISACA (2015), 'Global Cybersecurity Status Report', [Available Online] <http://www.isaca.org/pages/cybersecurity-global-status-report.aspx> as accessed on 12th October 2015

 [2]H M Government (2014), 'Cyber Security Skills - Business perspectives and Government’s next steps', [Available Online] <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/289806/bis-14-647-cyber-security-skills-business-perspectives-and-governments-next-steps.pdf> as accessed on 12th October 2015

[3] Bada, M., Sasse, A., & Nurse, J. R. (2014). Cyber Security Awareness Campaigns: Why do they fail to change behaviour?. Report). Global Cyber Security Centre.

[4] Klopfer, E., Osterweil, S., & Salen, K. (2009). Moving learning games forward.

[5] Adams, M., & Makramalla, M. (2015). Cybersecurity Skills Training: An Attacker-Centric Gamified Approach. *Technology Innovation Management Review*, *5*(1).

**Additional equipment required. A laptop and data projector, whiteboard and/or flipchart and connection to the internet will be supplied as standard. If you need any additional equipment, please enter the details here:**

Laptop and data projector

**Section 3: Presenter details
please list all co-presenters**

|  |  |  |  |
| --- | --- | --- | --- |
| Title:Dr. | Given name(s):Chitra | Family name:Balakrishna | Job title:Senior Lecturer |
| Institution/Organisation: Edge Hill UniversityAffiliation:  | HEA Fellowship reference no:FHEA |
| Email address: balakris@edgehill.ac.uk | Twitter name: Chitra\_garge |

|  |  |  |  |
| --- | --- | --- | --- |
| Title:Prof.  | Given name(s):Daniela | name:Romano | Job title:Professor |
| Institution/Organisation: Edge Hill UniversityAffiliation:  | HEA Fellowship reference no: |
| Email address: Daniela.Romano@edgehill.ac.uk | Twitter name:  |

|  |  |  |  |
| --- | --- | --- | --- |
| Title:Mr | Given name(s):James | name:Coleman | Job title:Senior Lecturer |
| Institution/Organisation: Edge Hill UniversityAffiliation:  | HEA Fellowship reference no:FHEA |
| Email address: James.Coleman@edgehill.ac.u | Twitter name:  |